TECHNICAL DOCUNMENT 3316
February 2017

Standardized and Repeatable Technology Evaluation for Cybersecurity Acquisition

Roger A. Hallman
Jose Romero-Mariona
Maxine Major
Megan Kline
Lawrence Kerr
Geancarlo Palavicini
John San Miguel
Josiah Bryan

SSC Pacific
San Diego, CA 92152-5001

SSC Pacific
San Diego, California 92152-5001

K. J. Rothenhaus, CAPT, USN
Commanding Officer

C. A. Keeney
Executive Director

ADMINISTRATIVE INFORMATION

The work described by the Network Security Engineering Services and Operations Branch (Code 58230) of the Computer Network Defense-Cyber Security Division (Code 58200), SSC Pacific, San Diego, CA. The SSC Pacific Naval Innovative Science and Engineering (NISE) Progam provided funding for this Applied Research and Technology Transition project.

Released by
J. Romero-Mariona, Head
Network Security Engineering Services and
Operations Branch

Under authority of
E.J. Huffstetler, Head
Information Assurance Division

EXECUTIVE SUMMARY

Cybersecurity is a growing concern for the U.S. Government, indeed the U.S. is on the receiving end of an estimated 100,000 cyber-attacks each day. Cybersecurity is a fast-growing market where technologies are constantly evolving to counter threats to information and operational systems. Across the U.S. Government as a whole, there is no standardized and repeatable methodology for evaluating cybersecurity technologies. In this report, we introduce the Department of Defense (DoD)-centric and Independent Technology Evaluation Capability (DITEC), an experimental decision support service within the U.S. DoD which aims to provide a standardized framework for cybersecurity technology evaluations in support of acquisition decision making. In addition to DITEC as a proof-of-concept, we describe a family of services that include: DITEC+, an enterprise-level tool, and the Cyber-Supervisory Control and Data Acquisition (SCADA) Evaluation Capability (C-SEC), an instantiation of DITEC for evaluating SCADA network cybersecurity technologies.

CONTENTS

Figures

Tables

1. INTRODUCTION

Cybersecurity is a growing concern for the U.S. Government, indeed the U.S. is on the receiving end of an estimated 100,000 cyber-attacks each day [1]. Cybersecurity technology is a fast-growing market where technologies are constantly evolving to counter threats to information and operational systems. Cybersecurity investment processes for private and public sector organizations vary considerably —government agencies are often constrained by long-term budgetary and acquisition procedures while private sector organizations can make purchasing and policy decisions with considerably more ease [2]. Across the U.S. Government as a whole, there is no standardized and repeatable methodology for evaluating cybersecurity technologies. As a consequence, the cybersecurity acquisition process inevitably leads to duplicated efforts on the part of technical and acquisition personnel. Moreover, lessons learned within one sector of the government are not easily shared with others, which may lead to multiple agencies adopting a cybersecurity technology that fails to meet their needs [3]. In certain sectors of the government, where personnel are rotated through on a regular basis, cybersecurity policies and products may be replaced with each change in project supervision. A practical and important consequence of this is that cybersecurity acquisition decisions will be made by security non-experts. If an expert in a security topic leaves a team, their institutional knowledge on that topic may be lost. Knowledge that was common sense in previous decision-making efforts is not obvious to new teams.This situation introduces unacceptable risks such as the following:

- The decision to acquire a new technology or product may involve outdated knowledge, due to the quickly evolving nature of cybersecurity technologies
- Chosen products or technologies may not be the optimal choice for a system's security needs
- Network administrators must learn to use the new products which have been acquired.

We describe the Department of Defense (DoD)-centric and Independent Technology Evaluation Capability (DITEC), a U.S. Department of the Navy research project which aims to rectify these problems and provide decision support for cybersecurity acquisition professionals, and its family of software products. DITEC and its family of products offer a standardized and repeatable platform for performing and preserving technology and product evaluations, yet incorporate the flexibility to score products for use in different contexts. The rest of this work is organized as follows: Section 2 discuses policies and procedures for cybersecurity acquisition; Section 3 describes DITEC in depth; Section 4 describes DITEC+, an enterprise-ready implementation of DITEC; Section 5 describes an instantiation of DITEC+ used for evaluating cybersecurity technologies in an operational technology environment as well as in-depth descriptions of features and functionality; Sections 6 and 7 cover future work and concluding remarks, respectively.

2. CYBERSECURITY TECHNOLOGY ACQUISITION: POLICY AND PROCEDURE

Billions of dollars are invested in cybersecurity technology each year [4]. This money is spent on procurement, maintenance, retirement, and replacement of these products. The acquisition process is often inefficient, resulting in increased costs for a delayed product that may not adequately meet the security needs of the organization.

2.1 THE DECISION TO PROCURE

In large organizations, the decision to procure a cybersecurity solution is often driven by requirements rather than by an observed specific need. Conversely, once a real need for a solution appears it may not be clearly supported by a defined requirement. Furthermore, requests which are not clearly supported by requirements in the organization's chosen framework may not be supported by senior management and the burden to prove its necessity will rest with the chief information security officer (CISO) or other information security managers.

Many organizations use the NIST[1], ISO-27000[2], or COBIT frameworks[3], but for smaller organizations, these frameworks can be overly complex and may not meet the organization's perception of risk. As such, the need for a cyber solution may be even more ambiguously supported by the adopted requirements.

Once a cyber solution is identified as needed by information security personnel (even if funding is available) the procurement request is likely to meet resistance from senior management if they believe the organization does not have the staffing or experience necessary to execute the solution. A lack of experience or personnel may also drive a department to not adopt a technology if they feel that its capabilities might be greater than their own capabilities to fully understand the solution, even if it is adequate to meet their needs. A lack of mature return on investment (ROI) models for cybersecurity leaves some departments scrambling to research financial data if their organization is more concerned with proving a financial benefit for adopting a cybersecurity technology.

2.2 TECHNOLOGY SELECTION

Often organizations will adopt frameworks (e.g., NIST, ISO-27000, or COBIT) to drive cybersecurity decision making. These frameworks do benefit organizations, as it has been shown that the lack of an adopted a framework correlates to underspending on cybersecurity. However, not all cyber acquisition can be easily defined or addressed by the requirements of that adopted framework [2].

Government agencies, which are heavily compliance-driven, do well in identifying the need for cyber acquisition but not in identifying the best technology to meet that need [2]. Despite the vast sums of money spent on cybersecurity, there is no standardized method to assist cybersecurity personnel in choosing the most appropriate products to secure their systems [3]. The focus is often more on checking boxes than evaluating cyber risks.

Once a technology type is identified, it is still very difficult to determine which vendor product will perform most efficiently without performing a bulk comparison of technologies against each other. Often, organizations will start the comparison via third-parties such as Gartner[4] or Forrester[5] [2], however not all

[1] https://www.nist.gov/cyberframework
[2] http://standards.iso.org/
[3] http://www.isaca.org/
[4] http://www.gartner.com/
[5] https://go.forrester.com/

organizations have the funding or resources to procure and set up each technology and test it against real-world threats just to make a purchasing decision. Moreover, not all organizations that have a need for a technology are qualified to determine how well one vendor's product performs against others.

2.3 VENDOR SELECTION

During an organization's decision-making process, vendors will often write project proposals for their own products—either those on the market or in development. This often results in the decision of which cybersecurity technology to purchase being inadvertently made by the vendors themselves.

The contract, which is detailed, extremely inflexible, and difficult to modify, requires the products listed in the vendor's proposal with little concern for emerging threats or those products' future performance. Once the proposal is accepted, the organization is limited to that vendor's product offering, even as the cyber domain changes. The capabilities selected are limited to only those the vendor can provide, and the vendor is required to produce only what is proposed. This forces the vendor to produce only contracted solutions rather than incorporating new technology to address new cyber threats. While contracts are being worked out, the organization is effectively limited in its capability to handle any new threats.

Additionally, vendor maturity is a limiting factor for technologies that can be considered for adoption. The U.S. General Services Administration's IT Schedule 70[6] requires that cybersecurity companies have at least two years of past performance for consideration as a vendor. This is a high bar that limits the ability of young cybersecurity companies to market the most up-to-date technologies and products to the government to mitigate current threats.

2.4 THE PURCHASE PROCESS

Procuring expensive technologies that involve vendor contracts introduces layers of paperwork and intentional technology transition delays; the process can be rather inflexible to address changing needs during the procurement process. According to Moore et al., "structural issues within the bureaucracy often inhibit adequate and timely prioritization" [2]. The US Government, in particular, requires a full technology acquisitions approval cycle of 3 years for any purchases over $3000. Purchases of $500,000 and up require Congressional approval. By the time these technologies have been purchased and deployed, the entire cyber threat domain has changed and the solution that was time consuming and costly to procure is now effectively outdated.

[6] http://www.gsa.gov/schedule70

3. DITEC AS A PROOF-OF-CONCEPT

The Department of the Navy funded the DoD-DITEC project (and following efforts) to create a tool to assist acquisitions personnel in purchasing already certified and accredited cybersecurity technology appropriate to their systems [3]. Engineers and IT personnel often have biased opinions, while managers who are non-security experts are likely to understand their security needs as explained by a vendor sales representative. DITEC standardizes the cybersecurity acquisition process in part by instituting guidelines and frameworks (e.g., NIST) Cybersecurity Framework, the DoD 8500 Series Information Assurance Controls[7]) to establish the types of procedures, controls, threats, and features that provide the test cases for which cybersecurity technologies would be evaluated. A market survey was conducted to learn what technologies were available for acquisition and to classify them into a three-tiered categorization based on their capabilities. Technology evaluation metrics and a scoring algorithm were developed by creating a taxonomy which matched technologies and test cases, allowing users to evaluate and make high-level comparisons of multiple technologies against one another.

DITEC consists of three components [3]:

1. Process – Evaluates a specific cybersecurity technology to determine how well it meets DoD/Navy needs.

2. Metrics – Measures how well each technology meets the specified needs across 125 different test cases.

3. Framework – Provides the format necessary to compare and contrast multiple technologies of a specific cybersecurity area.

Technologies were rated by metrics on three levels of granularity. The highest level of granularity is the "Capability" level. There are 10 of these Capabilities, which correspond to very broad ability categories (e.g., *Protect, Respond, Operations, Lifecycle Management*). The "Sub-Capability" level is the middle level of granularity, narrowing the focus from the Capability level (e.g., Protect—*Cryptographic Support*, Lifecycle Management—*Cost of Extended Vendor Support*). Finally, the "Sub-Capability Elements" level included very specific test cases.

[7] http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

4. DITEC+: A SCALABLE, ENTERPRISE-READY TECHNOLOGY EVALUATION CAPABILITY

DITEC served as a proof-of-concept but lacked the scalability required for further development and adoption. DITEC+ was then funded to resolve issues of scalability and create an enterprise-ready tool to aid in the acquisition process. Among the improvements to DITEC's proof-of-concept, DITEC+ improved on each of the three components:

1. Process—DITEC+ prescribes additional/customizable steps for focused evaluations pertaining to specific stakeholders and offers those steps as a library of evaluation guidelines.

2. Metrics—DITEC+ revised and improves on the DITEC metrics module to enable technologies to receive a "score" based on their evaluation performance against the metrics and provides the ability to apply "weights" to each evaluation per specific items of interest identified during the process. DITEC+ Metrics provide support for prioritizing results based on a variety of different aspects.

3. Framework—DITEC+ leverages the existing DITEC Framework but ensures that it is ready for enterprise-wide use, supporting multiple users and evaluations by adding robustness to the database and evaluation algorithms.

These and other improvements enable a DoD/Navy-centric, cost-effective and streamlined evaluation of various cybersecurity technologies that is defined by a process that is standardized, flexible, repeatable, scalable, and contains granular metrics (developed in-house with subject matter expert support). Additionally, DITEC+:

- Supports multiple and concurrent users and technology evaluations,

- Provides the ability to compare various cybersecurity technology evaluations,

- Integrated CAULDRON [5], a network vulnerability mapping tool,

- Developed new metrics for measuring differences across evaluations and technologies while estimating the level of cybersecurity provided,

- Developed a new ranking/prioritization mechanism of evaluated technologies based on user preferences [6], and

- Developed and integrated a recommender system to assist security non-experts in deciding which technologies best suit their situational needs [7].

4.1 PRIORITIZATION OF EVALUATIONS

Recognizing that personnel at different levels of an organization would have competing priorities, the User Priority Designation (UPD) [6] was developed to view evaluations in light of contextual priorities. For example, an agency's comptroller may place a heavier priority on the lifetime cost of a product, where a network administrator would be more concerned with the ability to install a vendor update with minimal system downtime.

The UPD tool uses a scalable weighting scheme to give certain capabilities (Capabilities, Sub-Capabilities, or Sub-Capability Elements) greater priority over others. This flexibility allows for cybersecurity acquisition decisions to be made with input from multiple levels—from system administrators who actively oversee network operations, to the management who are ultimately responsible for the overall health of an organization. For instance, a system administrator may prioritize certain security features as well as ease of product installation and use, while the chief financial officer is primarily concerned with the long-term cost of purchasing and maintaining that product. The UPD framework enables all stakeholders to accurately voice their priorities and concerns to reach optimal acquisition decisions.

The UPD works as follows, the user chooses a priority level for each capability and a weight is assigned to each capability based on the assigned priority. The priority levels rank from 0 to 5 as follows:

- UPD Rank 5 (Top Priority)
- UPD Rank 4 (High Priority)
- UPD Rank 3 (Moderate Priority)
- UPD Rank 2 (Low Priority)
- UPD Rank 1 (Minimal Priority)
- UPD Rank 0 (No Priority).

All N capabilities must be assigned to a UPD Level, and multiple capabilities may be assigned to the same level. When multiple capabilities are assigned to the same UPD Rank, a *Collision* occurs. Any capabilities given UPD level 0 are denoted as *Exclusions* and will not be weighted, thus there are $M = N - Exclusions$ positively weighted capabilities. There are then $n = M - Collisions$ weights to be assigned by the UPD. Finally, there are constants $m_0 = 0, m_1, ..., m_n$ which represent the number of capabilities to be weighted at each UPD Level.

Take the initial remaining weight $I_0 = 1$ and partition it into $J_0 = I_0/(m_0 + m_1)$ parts. The first weight $w_1 = J_0 + (J_0 \cdot (M - m_1)/M)$. From there we can recursively define

$$\begin{aligned} I_{i+1} &= I_i - m_{i+1} \cdot w_{i+1}, \\ J_i &= I_i/(m_0 + \cdots + m_{i+1}), \\ w_{i+1} &= J_i + (J_i \cdot (M - m_{i+1})/M). \end{aligned}$$

Figure 5 in Section 5.3 shows a graphical interpretation of user preferences versus evaluation “raw scores” through the use of the UPD tool.

Using DITEC+’s UPD framework, technology evaluations can be viewed by cybersecurity professionals and by management, allowing all stakeholders within the agency to project how various technologies and products will meet their needs according to differing criteria. It is often the case that cybersecurity non-experts will have a role in the acquisition decision making process and so we invented the Technology Matching Tool (TMT), a recommender system which helps to match users to the technology (or suite of technologies) which best match their needs [7, 13]. The TMT is discussed in greater detail in Section 5.3.1, in the context of cybersecurity for operational technology environments.

5. C-SEC: SUPPORTING CYBERSECURITY IN INDUSTRIAL CONTROL SYSTEMS AND CRITICAL INFRASTRUCTURE

Critical infrastructure (e.g., power grids, water treatment plants) have had a multitude of cyber-attack vulnerabilities discovered as they are becoming increasingly interconnected [8]. Supervisory Control and Data Acquisition (SCADA) systems [9], used in many automated processes including power generation and distribution, are of particular interest to cybersecurity researchers. These systems are notoriously fragile (e.g., timing sensitivities) and many cybersecurity products available on the market for Information Technology (IT) systems are inappropriate for SCADA systems [10]. The Cyber-SCADA Evaluation Capability (C-SEC) is an instantiation of DITEC+, designed specifically to test and evaluate the suitability of cybersecurity technologies for SCADA environments [11]. Security has not traditionally been a concern for SCADA systems because different manufacturers employed diverse protocols, however as protocols have become standardized this is no longer the case [12].

C-SEC supports cybersecurity decision making across new technologies by enabling a streamlined, flexible, and repeatable evaluation process against DoD-specific needs and requirements. Traditional security evaluations are expensive, requiring time and resources that smaller-scale projects cannot afford. Moreover, these evaluations tend to be non-repeatable and ultimately lack usability and applicability beyond just that one instance, thus jeopardizing their long-term ROI [3]. As an instantiation of DITEC+, C-SEC has three main components:

1. A software evaluation tool
2. A laboratory environment
3. An online, collaborative environment.

The software evaluation tool walks non-SCADA security experts through a quick, high-level evaluation process for determining the highlights of specific technologies of interest. The laboratory environment integrates the technology of interest into a prescribed configuration, which then provides a more detailed evaluation. Lastly, the online collaborative environment serves as a repository of past evaluations to facilitate reuse of results.

5.1 The C-SEC Software Evaluation Tool

The C-SEC Evaluation Tool is composed of DITEC's three main parts: a process, metrics, and a framework (Figure 1) [3, 11]. This approach provides not only the process necessary to determine if a certain technology meets DoD/Navy needs, but also provides the metrics to measure how well those needs are met and a framework to enable the comparison of multiple technologies of interest.

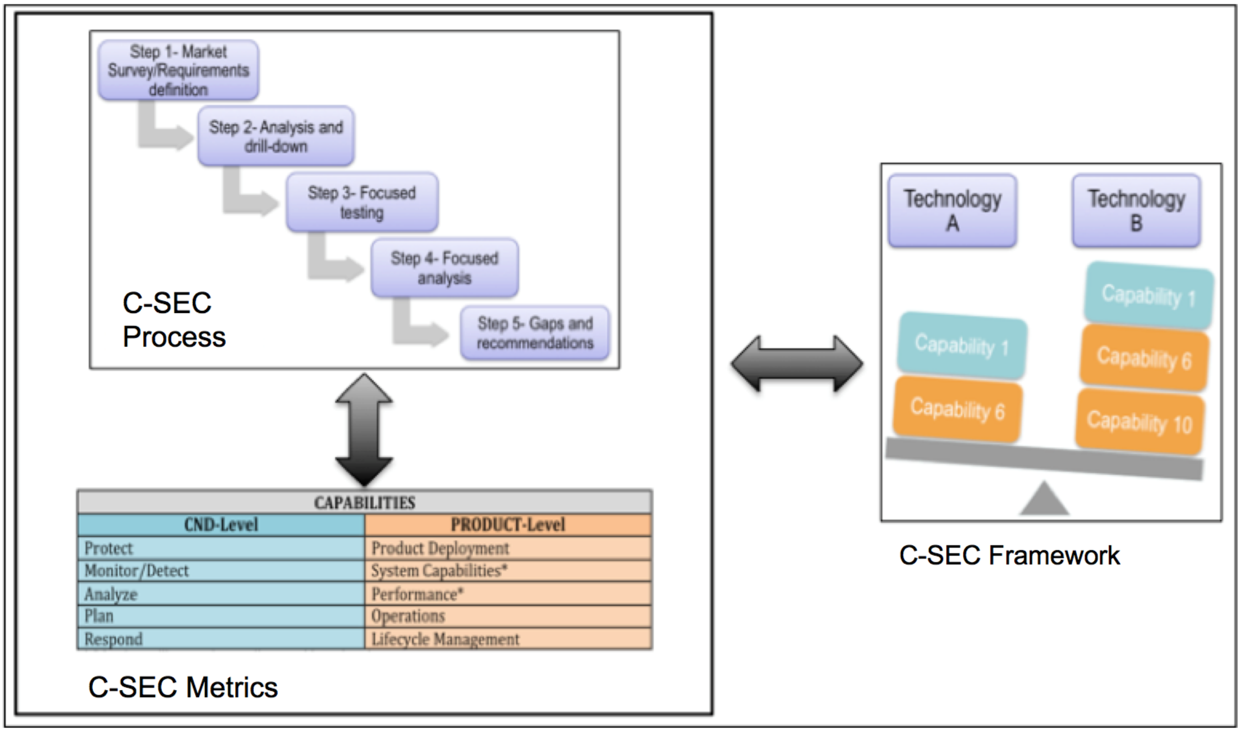

Figure 1. The C-SEC evaluation framework.

5.1.1 The C-SEC Software Evaluation Process

A software evaluation process is the first major step in the C-SEC approach to cybersecurity decision support. It's purpose is to evaluate a specific cybersecurity technology and determine if it meets (or not) DoD/Navy needs. This evaluation process involves the following five steps:

1. Market survey – High-level view of current offerings for the particular cybersecurity technology area of interest as well as a defined set of tests to determine the compatibility of those offerings with identified needs.

2. Analysis and drill-down – Results from the market survey are analyzed and the top percentage (varies based on each study, interest, and needs) of technologies will move down to the next step.

3. Focused testing – This step takes the technologies identified during the analysis, and drill-down to test them more rigorously by means of test cases that go beyond the high-level used during step 1. Often times a simulated test environment is built to test the functionality of the test subjects. In addition, documentation reviews are also used to determine if needs are met.

4. Focused analysis – This step evaluates the results for each technology tested in Step 3 and apply metrics to determine how well each need was met.

5. Gaps and recommendations – The analyzed results are used to determine current technology gaps and suggest recommendations for future research.

5.1.2 C-SEC Metrics

Metrics, and specifically those which are related to non-functional aspects, pose a difficult problem for cybersecurity analysis and decision makers.Traditional approaches to measuring are not well suited for aspects like security and usability [3]. Consequently, researchers, industry practitioners, and the government lack the appropriate tools to baseline and track specific characteristics of current technologies. C-SEC provides metrics support that is applicable for security and usability characteristics, and is relevant to academia, industry, and government sectors. Specifically, C-SEC provides metrics across three areas to make its results repeatable:

1. Metrics Discovery and Application – To develop DoD-specific security metrics and apply them to C-SEC Process results.

2. Metrics Manipulation – To enable manipulation and results integrity.

3. Metrics Visualization – To enables metrics traceability and decision making support.

5.1.2.1 Metrics Discovery and Application

Metrics must first be developed and their application to C-SEC results determined. To provide relevant metrics to a variety of cybersecurity technologies we have selected ten different metrics areas, referred to as Capabilities (Table 1). These Capabilities represent the highest level of granularity and cover aspects across two main areas, Computer Network Defense (CND) concepts as well as Product-Level. The CND-level metrics refer to the basic aspects related to security—that is, how well does a technology support the protection, monitoring and detection, analysis, planning, and response to threats or attacks. The Product-Level metrics refer to aspects more commonly associated with "day-to-day" operations of a technology. Product-Level metrics look at aspects that range from the cost and difficulty of deploying a specific technology to the complexity of maintaining that technology once it is deployed. Each type of metric applied to the results obtained from the application of the C-SEC Process is assigned a numerical value that reflects how well the specific technology under evaluation meets the objectives defined for that metric.

Table 1. C-SEC capabilities, divided between CND and product level.

Capabilities	
CND Level	Product Level
Protect	Product deployment
Monitor/detect	System capabilities*
Analyze	Performance*
Plan	Operations
Respond	Lifecycle management

5.1.2.2 Metrics Manipulation

C-SEC supports the manipulation of these metrics to better understand the technology under various shades of light. C-SEC employs a granular approach to metrics manipulation; this enables flexibility as well as reusability of results. For example, suppose that Agency 1 just completed an evaluation of Technology X with an emphasis on the cost, but now Agency 2 also wants to evaluate the same Technology X with a different emphasis on protection capabilities. Agency 2 could reuse the same C-SEC results that Agency 1 produced, and manipulate the C-SEC Metrics to put more weight into the protection aspects of the results (and less on the cost aspects) to obtain a different measurement of technology X's ability to meet those needs.

C-SEC Metrics prescribe two new levels in addition to the Capability-level described in Section 5.1.2, which further break down each Capability into Sub-Capabilities, and those into Sub-Capability Elements. This granular approach prescribes a few rules:

- Every Capability is composed of one or more Sub-Capabilities
- Every Sub-Capability is composed of one or more Sub-Capability Elements
- Sub-Capability Elements can be duplicated across other Sub-Capabilities.

To illustrate this, Figure 2 shows how a Capability, like Protection, is composed of two Sub-Capabilities: Vulnerability Protection and Listing (which refer to two possible ways to achieve protection). These are further broken into Sub-Capability Elements, such as Vulnerability Scanning and Vulnerability Reporting (which refer to two possible ways to achieve Vulnerability Protection).

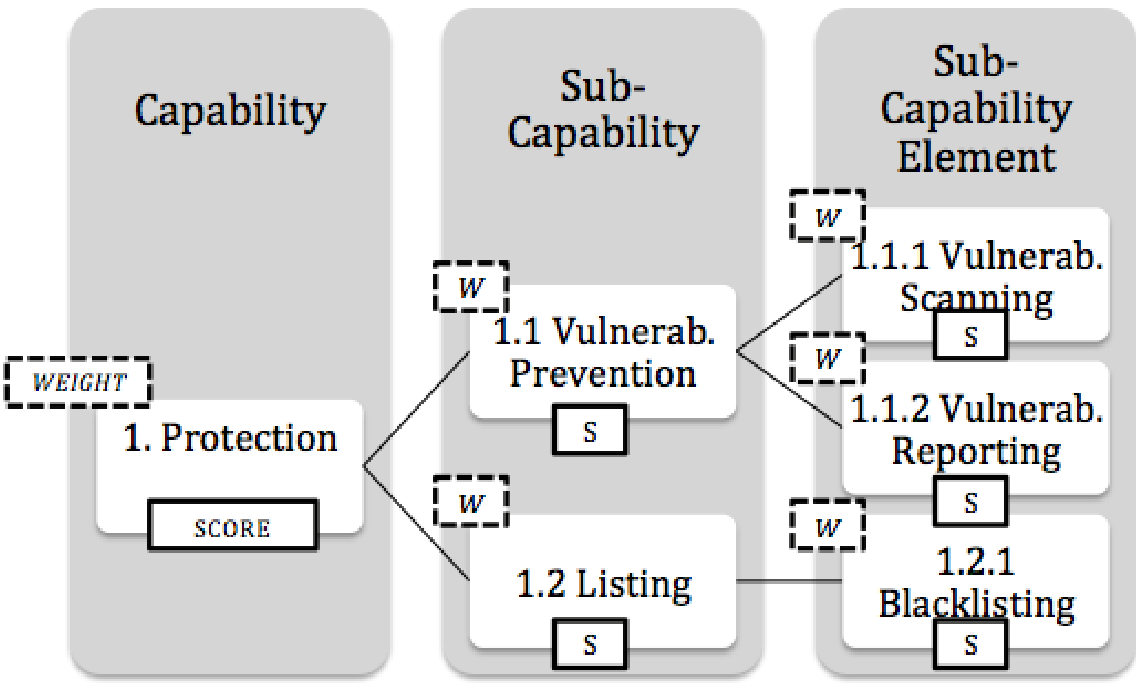

Figure 2. C-SEC metric granularity.

C-SEC computes an aggregated score from various levels of granularity (Capability $\rightarrow$ Sub-Capability $\rightarrow$ Sub-Capability Element) as well as provides "weights" at each element to facilitate the flexibility and reuse of the C-SEC Metrics. This granular system is what would enable Agency 2, in our earlier example, to take the C-SEC Process results from Agency 1 and apply different weights to their scores to emphasize different aspects of interest.

5.1.2.3 Metrics Visualization

The final aspect supported by C-SEC Metrics is visualization (Figure 3). C-SEC metrics provide a visualization for the manipulation of the various scores and weights applied to the C-SEC process results so that users can see in real-time the effect that changes have on the original results. The metrics visualization component is mainly driven by C-SEC's graphical user interface (GUI) and changes made to the original results are stored in a database. Finally, the visualization of C-SEC metrics also supports decision making by employing Bayesian-network models to provide probabilities as well as ROI information.

Figure 3. C-SEC evaluation results.

5.1.3 C-SEC Framework

The C-SEC Framework provides the format necessary to compare and contrast multiple technologies of a specific cybersecurity area. Furthermore, the framework also supports a repository of past and present evaluation results to facilitate reuse. The C-SEC Framework serves as the key component of the online collaborative environment (to be discussed in Section 5.3), through which various users can share results and reuse information. While C-SEC applications are individually installed by users (clients), the framework serves as the hub (server) that connects them together.

5.2 The C-SEC Laboratory Environment

To give more meaningful evaluations, we developed the C-SEC Laboratory Environment. The C-SECLaboratory Environment consists of several SCADA demonstration kits from various vendors, which are easily reconfigurable to simulate different environments and are available from various vendors. Cyber security professionals can use this setup to investigate, the Technology Under Evaluation (TUE) for a much more detailed evaluation beyond just the C-SEC software tool. Laboratory assets include:

- SCADA and ICS components including, but not limited to programmable logic control units (PLCs), networking equipment, valves, actuators, motors, and various other components, which create a realistic industrial environment, these components are representative of what is offered by the major SCADA and ICS suppliers
- A DoD-mandated vulnerability scanner
- A vulnerability visualization tool called Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks (CAULDRON) [6]
- A suite of internally developed, custom security test scripts to exercise the equipment beyond normal operation parameters.

CAULDRON, developed by George Mason University, is a network vulnerability visualization tool that takes vulnerability scan results in `.xml` format, parses them, and outputs a weighted network diagram [5]. The nodes represent the Internet Protocol (IP) addresses within the network and the edges show potential for information exchange. Each edge has an associated weight that represents the number of vulnerabilities between connected nodes and shows how they propagate throughout the network. This tool was designed to enable network modeling; a user could visualize their existing network, then model how a security product would change the state of the network based on placement. A set of scripts was developed to automate a number of well-known approaches to network penetration. These scripts are deployed on the SCADA network to test the effectiveness of security products, see Figure 4.

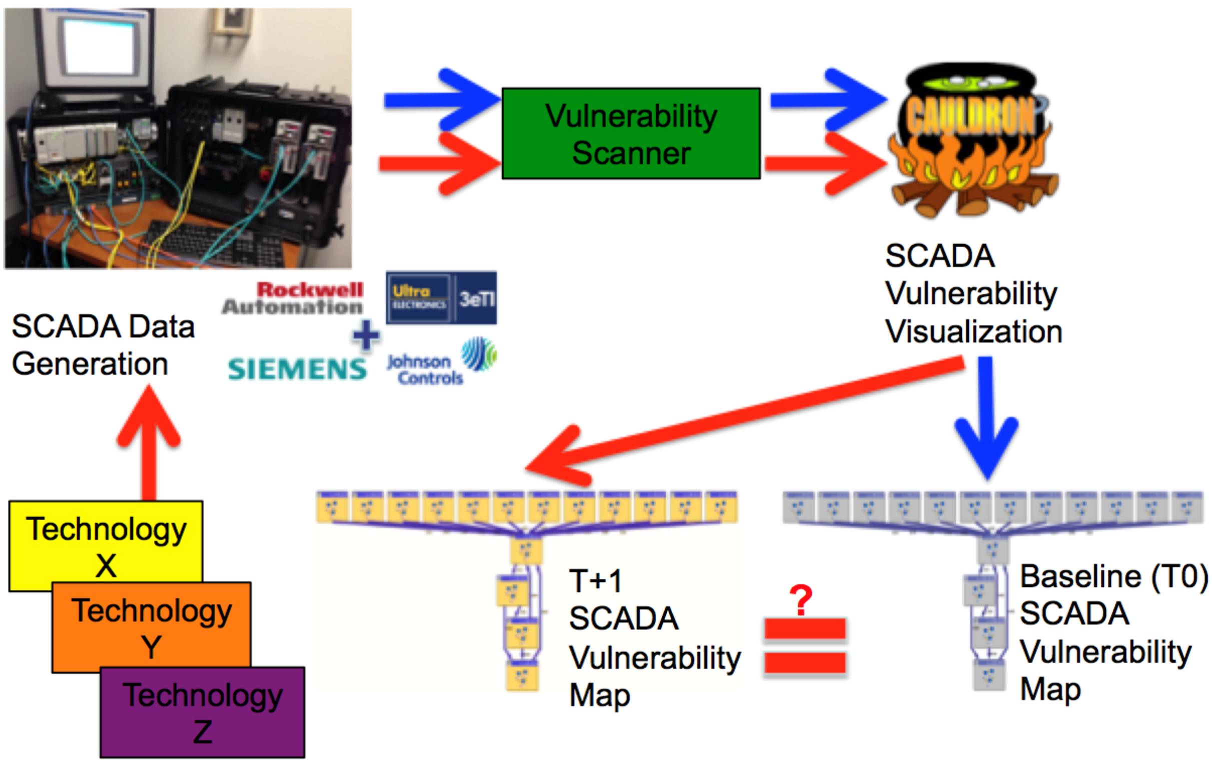

Figure 4. The C-SEC Laboratory Evaluation Process

The C-SEC process for testing the effectiveness of security technologies is as follows (Figure 4):

1. A baseline vulnerability scan of SCADA equipment is performed
2. The TUE is installed and configured
3. Equipment is run for several weeks to generate data
4. SCADA equipment is re-scanned
5. Scan results are visualized using CAULDRON
6. A comparison of the baseline vulnerability scan and re-scan determines the effectiveness of the TUE
7. Internally developed security test scripts are performed to validate scan results.

5.3 The C-SEC Online Collaborative Environment

The C-SEC Online Collaborative environment consists of a web application providing users with an interface to create, search, and reuse standardized evaluations of security technologies that are specifically marketed for SCADA networks. This online collaborative environment was created to standardize what is currently a disparate process for evaluating security technologies and apply a set of weights that is representative of user needs. Users have the option to perform new evaluations or choose previously completed evaluations. Allowing users to choose existing evaluations enables them to make informed decisions about which technology (or suite of technologies) to implement on their networks. The online environment is designed for easy deployment to both enterprise and tactical networks. To achieve this goal, C-SEC deploys virtual machines (VM) that are lightweight and can to be hosted in almost any environment.

One of the most valuable sources of information for choosing security controls is peer feedback, and as such an overarching goal for C-SEC is the development of a repository of evaluations for reuse [10]. When a user wants to reuse an existing evaluation, they have two options. They can take another user's evaluation at face value; they are satisfied with the answers provided by the other user and accept the score. Alternatively, they can reuse existing evaluations while overlaying a set of weights based on individual needs using the built-in wizard to establish their preferences [6]. Weights based on an individual's prioritization are overlaid onto the existing evaluation data. The user also sees a visualization consisting of a bar graph of existing scores over each of the Capabilities and an overlay "wave" of their weighted preferences. This allows users to directly compare their priorities to what the technology provides according to the existing evaluation, shown in Figure 5.

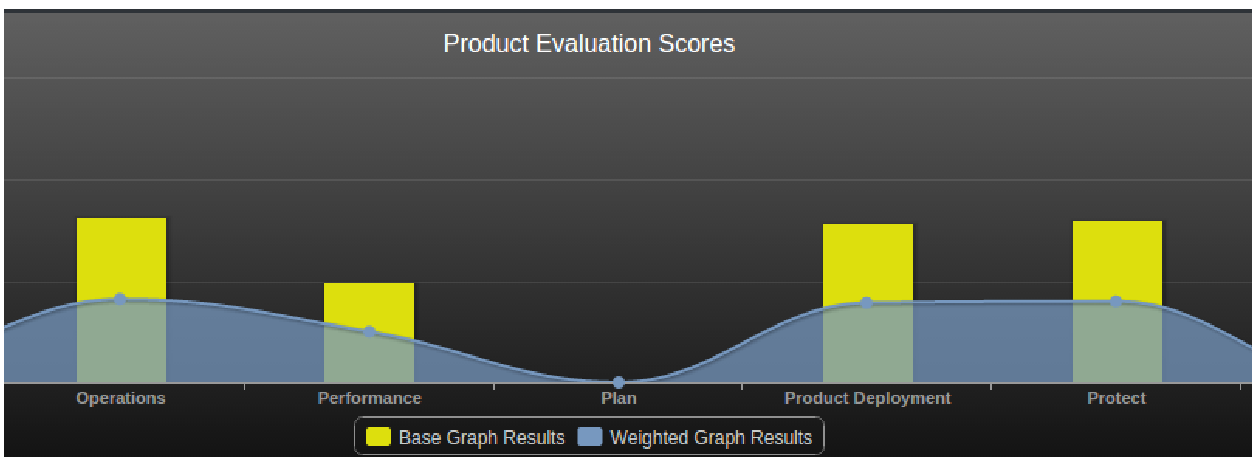

Figure 5. The C-SEC "Wave" Overlay comparing user priorities with existing evaluations.

5.3.1 The Technology Matching Tool: A Recommender System for Security Non-Experts

A Technology Matching Tool (TMT) was implemented in C-SEC's Online Collaborative Environment as a recommender system to assist security non-experts make acquisition decisions when determining the cybersecurity technologies that best suit their needs [13]. The TMT makes use of the UPD introduced in Section 4.1. The Sub-Capabilities described in Section 5.1.2 offer enough specificity to direct a user to specific technology. The TMT uses this feature, along with the Sub-Capability Element use cases, to recommend cybersecurity technologies that are appropriate to the network in question. There are two phases to the TMT:

1. Sub-Capability Prioritization – different Sub-Capabilities will have differing levels of importance with changing context. The TMT uses the UPD framework (with a less developed weighting scheme) to assign weights according to the Sub-Capability's priority in a given context.

2. Use Case Specification – use cases, in the form of Sub-Capability Elements, are determined.

The user assigns a priority level according to the UPD framework to the (currently 44) Sub-Capabilities that C-SEC uses. These Sub-Capabilities are weighted according to their assigned priority (e.g., a Sub-Capability with a UPD rank of 5 will have a weight of 1.00, while a Sub-Capability with a rank of 3 will have a weight of 0.55). The use case context requirements are specified by the user completing a series of yes/no questions based on the (currently 109) Sub-Capability Elements.

Each cybersecurity technology evaluated for C-SEC receives a Sub-Capability Element profile which is "vectorized". This gives a binary "Product Vector" where, in the event that the technology performs a Sub-Capability Element use case the corresponding vector element is a 1, and a 0 otherwise. Correspondingly, a binary "User Requirement Vector" is derived from the yes/no questionnaire that was used to specify contextual use case requirements. The vector elements are weighted according to the priority weighting of their corresponding Sub-Capability Elements, that receive a weight according to their Sub-Capability. A weighted Euclidean Metric is then used to match the user with the technologies that best suits their determined needs [14].

The TMT's basic functionality can be modified to improve the user experience. For example, a Sub-Capability receiving a UPD rank of 0, may have its associated use cases disregarded in the Use Case Specification phase. Figure 6 displays the TMT's results for single technologies, but the TMT can recommend suites of cybersecurity technologies that will work in concert to meet the network's contextual requirements (Figure 7).

Figure 6. The C-SEC TMT, offering single technology recommendations based on Sub-Capability Prioritization and Use Case Specification.

Figure 7. The C-SEC TMT, offering technology suite recommendations based on Sub-Capability Prioritization and Use Case Specification.

6. FUTURE WORK

DITEC was a proof-of-concept that provided an early exploration at cybersecurity metrics, objective evaluations, and re-usability of such evaluations. While still experimental systems, DITEC+ and C-SEC became much more mature projects which enabled actual evaluations of cybersecurity products and developed tools for comparing their results. For the DITEC process to have a broader impact, it must be transitioned from an experimental program to a “Program of Record” to guide cybersecurity acquisition across agencies. This transition would ultimately enable not just a wider adoption, but lead to a standardization of cybersecurity metrics and evaluations across the government sector. Larger private institutions such as banks or chain retailers may also benefit from the adoption of DITEC’s process, metrics, and recommendations for successful deployments.

Continuing work is underway to make the DITEC family suitable for larger adoption, including the following:

- Further development of metrics and test cases to evaluate “active” cybersecurity and counterintelligence technologies (e.g., honeypots)
- Development of instances of DITEC+ for environments beyond the enterprise and SCADA environments (e.g., IoT and Fog Computing environments)
- Study into how DITEC process results can be turned into actionable plans that could enable much more automated cyber defenses
- Enhance the DITEC and C-SEC concepts with ROI as it relates to specific areas of interest (e.g., energy, internet of things (IoT), etc)
- Human factors evaluation study to improve the user experience as well as the overall usability of the processes and tools.

The UPD and TMT show promise in helping determine the ROI of cybersecurity acquisition decisions. A challenge of understanding ROI for cybersecurity is that it is difficult to quantify. There are many reasons for this optimism. For instance the impact of purchasing and integrating a technology must be weighed against hypothetical circumstances as well as potentially outdated information regarding current states. Many decision makers see ROI for cybersecurity as either impossible to calculate or simply do not factor it into their acquisition decisions [2]. With some modification, the TMT could be used to illustrate ROI of cybersecurity technologies against monetized impacts.

We are working on “light”/mobile versions of our tool sets to enable evaluations to happen where the systems are, rather than just in our laboratory setting. We expect this an area will eventually expose our work to new opportunities and requirements.

Beyond the current plans for enhancing current process and tools such as UPD and TMT, we foresee a need to expand and generalize our approach to become applicable to other important areas like safety and privacy. The ability to not only make better-informed decisions that matter today, but also enable modeling of future effects of such decisions is important for future work. One of the challenges we currently face is the general aversion to improvements that seem like standards (and/or the attempt to standardize something) in the age where prototyping (i.e., failing early and often) reigns. We understand this challenge and seek to continue the development of our processes and tool sets to go beyond simply pointing at something as right or wrong, but enabling users to make actionable decisions that are reusable.

7. CONCLUSION

The U.S. Government faces difficult obstacles with respect to cybersecurity technology acquisition. Some of these problems relate to the rigidity of budgetary cycles, which plan several years in advance and require significant effort to alter. Limited funds to support training and workforce development often mean sending a single employee to training and having them return to train their colleagues on what they have just been taught. Other acquisition policies make purchasing newly developed technologies, that could effectively defend against emerging threats, virtually impossible. These difficulties, particularly the long-term budgeting and acquisition cycles, make the government an attractive potential customer for cybersecurity technology companies, and many have sales teams (often composed of retired government personnel) specializing in public sector customers. This situation can lead to a “fog of more” situation where cybersecurity acquisition decisions are made with an avalanche of inadequate information.

Even seasoned IT professionals may have incomplete knowledge or biased opinions that hinder the effectiveness of cybersecurity acquisition. DITEC and its family of products provide acquisition decision support for cybersecurity technologies and products that have received certification and accreditation. DITEC and its follow-on works, DITEC+ and C-SEC, demonstrate the ability to mitigate this problem by building a technology evaluation process and tool that is standardized and repeatable. DITEC+ and its instantiations offer the ability to store and reuse product evaluations, weighted to reflect individual priorities. Institutions with higher personnel turnover will suffer a loss of institutional knowledge, possibly leaving acquisitions decisions to be made by cybersecurity non-experts. A TMT works as a recommender system that assists security non-experts to the technologies that will best meet the needs of their networks.

REFERENCES

1. M. Maloney. 2015. "Pentagon's DC3I Memo Acknowledges Thousands of Cyber Breaches that Compromised DoD Systems and Commits to New Cyber Culture." Available online at http://www.governmentcontractinsider.com/pentagons-dc3i-memo-acknowledges-thousands-of-cyber-breaches-that-compromised-dod-systems-and-commits-to-new-cyber-culture/. Accessed on February 10, 2017.

2. T. Moore, S. Dynes, and F. R. Chang. 2015. "Identifying How Firms Manage Cybersecurity Investment," *Southern Methodist University*. Available online at http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf. Accessed on February 10, 2017.

3. J. Romero-Mariona. 2014. "DITEC (DoD-Centric and Independent Technology Evaluation Capability): A Process for Testing Security." *Proceedings of the Software Testing, Verification and Validation Workshops (ICSTW), IEEE Seventh International Conference* (pp. 24–25). March 31–April 4, Cleveland, OH.

4. S. Morgan. 2016. "Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020," Available online at http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#1ef75ba876f8. Accessed on February 10, 2017.

5. S. Jajodia, S. Noel, P. Kalapa, M. Albanese, and J. Williams. 2011. "CAULDRON Mission-Centric Cyber Situational Awareness with Defense in Depth." *Proceedings of the 2011 IEEE - MILCOM 2011 Military Communications Conference* (pp. 1339–1344). November 7–10, Baltimore, MD.

6. R. Hallman, J. Romero-Mariona, M. Kline, and J. San Miguel. 2014. "DITEC User Priority Designation (UPD) Algorithm: An Approach to Prioritizing Technology Evaluations." DTIC Technical Document 3288 (December). Space and Naval Warfare Systems Center Pacific, San Diego, CA.

7. R. Hallman and B. Coronado. 2016. "DITEC Technology Matching Tool (TMT)." Technical Report 3021 (August), Space and Naval Warfare Systems Center Pacific. San Diego, CA.

8. F. Caldeira, T. Cruz, P. Simões, and E. Monteiro. 2015. "Towards Protecting Critical Infrastructures." In *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, pp. 121–165. Austin DeMarco, Ed. Information Science Reference, Hershey, PA.

9. Boyer, S. A. 2009. *SCADA: Supervisory Control and Data Acquisition*. 4th ed. The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

10. J. Romero-Mariona, M. Kline, and J. San Miguel. 2015. "C-SEC (Cyber SCADA Evaluation Capability): Securing Critical Infrastructures." *Proceedings of the IEEE International Symposium, Software Reliability Engineering Workshops (ISSREW)* (p. 38). November 2–5, Gaithersburg, MD.

11. J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr. 2016. "Security in the Industrial Internet of Things: The C-Sec Approach." *Proceedings of the International Conference on Internet of Things and Big Data* (pp. 421–428). April 23–25, Rome, Italy.

12. V. M. Igure, S. A. Laughter, and R. D. Williams. 2006. "Security Issues in SCADA Metworks," *Computers & Security*, *25*(7):498–506.

13. R. M. Jose, L. Kerr, R. Hallman, B. Coronado, J. Bryan, M. Kline, G. Palavicini, M. Major, and J. San Miguel. 2016. "TMT: Technology Matching Tool for SCADA Security," *Springer*, New York, NY.

14. J. M. Merigó, and M. Casanovas. 2011. "Induced Aggregation Operators in the Euclidean Distance and Its Application in Financial Decision Making," *Expert Systems with Applications*, *38*(6):7603–7608.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-01-0188*

1. REPORT DATE *(DD-MM-YYYY)*
February 2017

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE

Standardized and Repeatable Technology Evaluation for Cybersecurity Acquisition

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHORS

Roger A. Hallman
Jose Romero-Mariona
Maxine Major
Megan Kline
Lawrence Kerr
Geancarlo Palavicini
John San Miguel
Josiah Bryan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SSC Pacific
53560 Hull Street
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TD 3316

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

SSC Pacific
Naval Innovative Science and Engineering (NISE)
53560 Hull Street
San Diego, CA 92152-5001

10. SPONSOR/MONITOR'S ACRONYM(S)

SSC Pacific NISE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cybersecurity is a growing concern for the United States Government, indeed the United States is on the receiving end of an estimated 100,000 cyber-attacks each day. Cybersecurity is a fast-growing market where technologies are constantly evolving to counter threats to information and operations systems. Across the U.S. Government as a whole, there is no standard and repeatable methodology for evaluating cybersecurity technologies. In this document, we introduce the Department of Defense (DoD)-centric and Independent Technology Evaluation Capability (DITEC), an experimental decision support service within the DoD, which aims to provide a standardized framework for cybersecurity technology evaluations in support of acquisition decision making. In addition to DITEC as a proof of concept, we describe a family of services including DITEC+, an enterprise-level tool, and the Cyber-SCADA Evaluation Capability (C-SEC), an instantiation of DITEC for evaluating SCASA network cybersecurity technologies.

15. SUBJECT TERMS

Cybersecurity; cyber-attacks; DITEC; procurement; technology acquisition; technology selection; purchase process; enterprise-ready technology evaluation capability; C-SEC; cybersecurity in industrial control systems; critical infrastructure

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Roger A. Hallman
					19B. TELEPHONE NUMBER *(Include area code)*
U	U	U	U	27	(619) 553-7905

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

INITIAL DISTRIBUTION

84300	Library	(1)
58230	R. Hallman	(1)
58230	J. Romero-Mariona	(1)
58230	M. Major	(1)
58230	M. Kline	(1)
58230	L. Kerr	(1)
58230	G. Palavicini	(1)
58230	J. San Miguel	(1)
58230	J. Bryan	(1)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (1)

Approved for public release.

SPAWAR
Systems Center
PACIFIC

UNITED STATES NAVY

SSC Pacific
San Diego, CA 92152-5001